



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/498,716 | 02/07/2000 | Arjen K. Lenstra | 0225-4188 | 9213 |

7590 04/05/2004

Morgan & Finnegan, L.L.P.
345 Park Avenue
New York, NY 10154

| |
|----------|
| EXAMINER |
|----------|

HENEGHAN, MATTHEW E

| | |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2134

DATE MAILED: 04/05/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/498,716

Applicant(s)

LENSTRA ET AL.

Examiner

Matthew Heneghan

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10 March 2004.
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 25-56 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) 25-56 is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on 07 February 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. In response to the first office action, applicant has amended claims 25, 26, 32-34, 37, 40-42, 48-50, and 56. Claims 25-56 have been examined.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 27-32, 35-40, 48, and 51-56 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite in that they fail to point out what is included or excluded by the claim language.

Regarding claims 27-32, 35-40, and 51-56, these claims are omnibus type claims. For purposes of the prior art search, these claims are being considered to only include the limitations of their respective parent claims, and thus stand or fall with them.

These rejections may be overcome by adding limitations that either recite steps (in the case of methods) or components (in the case of systems) of the claimed inventions.

Regarding claim 49, it is unclear what purpose the claimed business has.

Claim 50 depends from rejected claim 49, and includes all the limitations of that claim, thereby rendering that dependent claim indefinite.

Regarding claims 32, 40, 48, and 56, the phrase "such as" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

3. In view of applicant's amendments, all other previous rejections under 35 U.S.C. 112 are withdrawn.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 25-32 and 49-56 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claimed matter solely teaches to the mathematical manipulation of an abstract idea. There is no tangible output to the method.

Although the claims now teach to systems containing memory, the limitations of the claims do not teach to the data being manipulated being tangibly embodied within that memory.

It is suggested that Applicant could overcome this rejection by adding a limitation wherein the generated public key were stored in the memory.

5. All other previous rejections under 35 U.S.C. 101 are withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 25-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over El Gamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory 31(4), 1985 in view of Brouwer et al., "Doing More With Fewer Bits," Advances in Cryptology - Asiacrypt '99, pp. 321-332 further in view of Lidl et al., "Introduction to Finite Fields and Their Applications," 1986, pp. 50-55.

El Gamal teaches a public key signature scheme based on discrete logarithms, and suggests that such a scheme can be extended from the $GF(p)$ to $GF(p^m)$. See part VI, "Conclusions and Remarks."

El Gamal does not disclose the conjugates and roots in such a case, or the order of the trace field employed.

Brouwer discloses a method using p^2-p+1 in $GF(p^6)$ (see section 3), and shows the derivation of the claimed roots (see section 3.3). The derivation of $F_g = X^3 - BX^2 + B^pX - 1$ is a function of the polynomial and roots.

Lidl teaches that trace fields can be extended from one to the other over normal bases.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the scheme of El Gamal by using the roots disclosed by Brouwer, and extending them to $GF(p^2)$, using the method disclosed by Lidl.

Response to Arguments

7. Applicant's arguments filed 10 March 2004 have been fully considered but they are not persuasive.

Regarding applicant's arguments to the rejections under 35 U.S.C. 103(a), see Paper No. 12, pp. 11-14, applicant is reminded that the achieving of $GF(p^6)$ security is not explicitly recited in the limitations of any of the claims, and it is therefore not necessary for any prior art to explicitly recite this ability.

Though ElGamal does suggest the use of values of 3 or 4 for m in p^m , given the amount of available computing power at the time the paper was written (1985). He also further states, however, that any value of m would be appropriate. There is no suggestion that the use of larger values of m would not be obvious. The remarks of the

final paragraph of ElGamal clearly do not teach away from the invention of the instant application.

Applicant further argues that the Diffie-Hellman variation disclosed by Brouwer does not disclose a public key system in $GF(p)$ that can be extended to any $GF(p^m)$. It is noted that it is well-known in the art that the Diffie-Hellman public key scheme is in $GF(p)$, and is extensible to powers of p .

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Art Unit: 2134

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (703) 305-7727. The examiner can normally be reached on Monday-Thursday from 8:00 AM - 4:00 PM Eastern Time. The examiner can also be reached on alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450

Or faxed to:


(703) 872-9306
Hand-delivered responses should be brought to Crystal Park 2, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

MEH



March 31, 2004



GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100